TECHNIQUE T858: UTILIZE/CHANGE OPERATING MODE

CyOTE Use Case(s)	MITRE ATT&CK for ICS® Tactic
Alarm Logs, HMI, Remote Login	Evasion, Inhibit Response Function
Data Sources	
Potential Data Sources	Packet Capture, Network Protocol Analysis, Device/Alarm Logs
Historical Attacks	Triton Attack at Petro Rabigh[1]

TECHNIQUE DETECTION

The Utilize/Change Operating Mode technique[2] (Figure 1) may be detected when a device's operating mode is changed without warning or reason.

To augment commercial sensor gaps, the CyOTE program has developed capabilities such as Proof of Concept tools[3] and Recipes[4] for asset owners and operators (AOO) to identify indicators of attack for techniques like Utilize/Change Operating Mode within their operational technology (OT) networks. Referencing CyOTE Case Studies[5] of known attacks, AOOs in both small and large organizations can utilize CyOTE's Use Case analyses to tie operational anomalies and observables to cyber-attack campaigns resulting in ever-decreasing impacts.

PERCEPTION: OBSERVABLES FROM HISTORICAL ATTACKS

The Utilize/Change Operating Mode technique was used in the Triton attack at Petro Rabigh in 2017.[6] In this attack, the following observables were identified:

- Increased internet traffic
- Increased DMZ traffic between information technology (IT) and OT networks

Disclaimer: Past occurrences are not guaranteed to occur in future attacks.

[1] MITRE, *Software: Triton, TRISIS, HatMan,* https://collaborate.mitre.org/attackics/index.php/Software/S0013
[2] MITRE ATT&CK for ICS, T858: Change Operating Mode, https://collaborate.mitre.org/attackics/index.php/Technique/T0858
[3] A Proof of Concept tool is a representative implementation of a set of steps and methods for identifying techniques. A Proof of Concept tool is defined as a script(code) or using capabilities of existing tools (e.g., Splunk, Gravwell), to demonstrate the capability to identify adversarial activity for a selected technique. A Proof of Concept tool is not ready for implementation in an AOO's environment as its major focus is to a specific instance (device, vendor, protocol, scenario) in order to prove a concept.
[4] A Recipe is a set of steps and methods for identifying techniques. Recipes can be used to develop a Proof of Concept or operational tool in an AOO's OT environment.
[5] Visit https://inl.gov/cyote/ for all CyOTE Case Studies.
[6] https://www.eenews.net/stories/1060123327

COMPREHENSION

In the Triton attack at Petro Rabigh, the adversary first gained access through an engineering workstation to map the network; once they gained control of the workstation, they moved through the network and deployed the malware, modifying operating modes and device logic to issue malicious command messages that shut down part of the plant.[7] By understanding the nature and possible origins of this attack, as well as how the adversary used the Utilize/Change Operating Mode technique to execute the attack, an AOO can better comprehend how this technique is used with others and enhance their capabilities to detect attack campaigns using this technique and decrease an attack's impacts.

CURRENT CAPABILITY

The CyOTE Proof of Concept tool actively queries a GE D60 to check the operating mode status and produce an alarm if the status changes.

POTENTIAL ENHANCEMENTS

Additional research is needed to tailor the CyOTE Proof of Concept tool to detect and track modifications to the operating state of supported devices. The Proof of Concept tool will be capable of querying a device directly or monitoring the network traffic to detect commands sent to change the operating mode. If the Proof of Concept tool detects modifications to the operating mode, it will output a customizable alert message.

ASSET OWNER DEPLOYMENT GUIDANCE

The finalized operational tool would support multiple deployment methods. To support a deployment method for network monitoring, the operational tool will need to be installed on a host which is able to observe the network traffic of devices to be monitored, such as a network span port. The second deployment method will include either installing the operational tool directly on a device to be monitored or installing the tool on a separate system and then configuring the tool with the remote access information including credentials.

AOOs can refer to the CyOTE Technique Detection Capabilities report (visit https://inl.gov/cyote/) for more information on the background and approach of CyOTE's technique detection capabilities.

AOOs can also refer to the CyOTE methodology for more information on CyOTE's approach to identifying anomalies in an OT environment, which, when perceived, initiates investigation and analysis to comprehend the anomaly.

Click for More Information	CyOTE Program || Fact Sheet || CyOTE.Program@hq.doe.gov
DOE Senior Technical Advisor	Edward Rhyne || Edward.Rhyne@hq.doe.gov || 202-586-3557

[7] CyOTE Case Study: Triton in Petro Rabigh. https://inl.gov/wp-content/uploads/2021/09/Triton-CyOTE-Case-Study.pdf

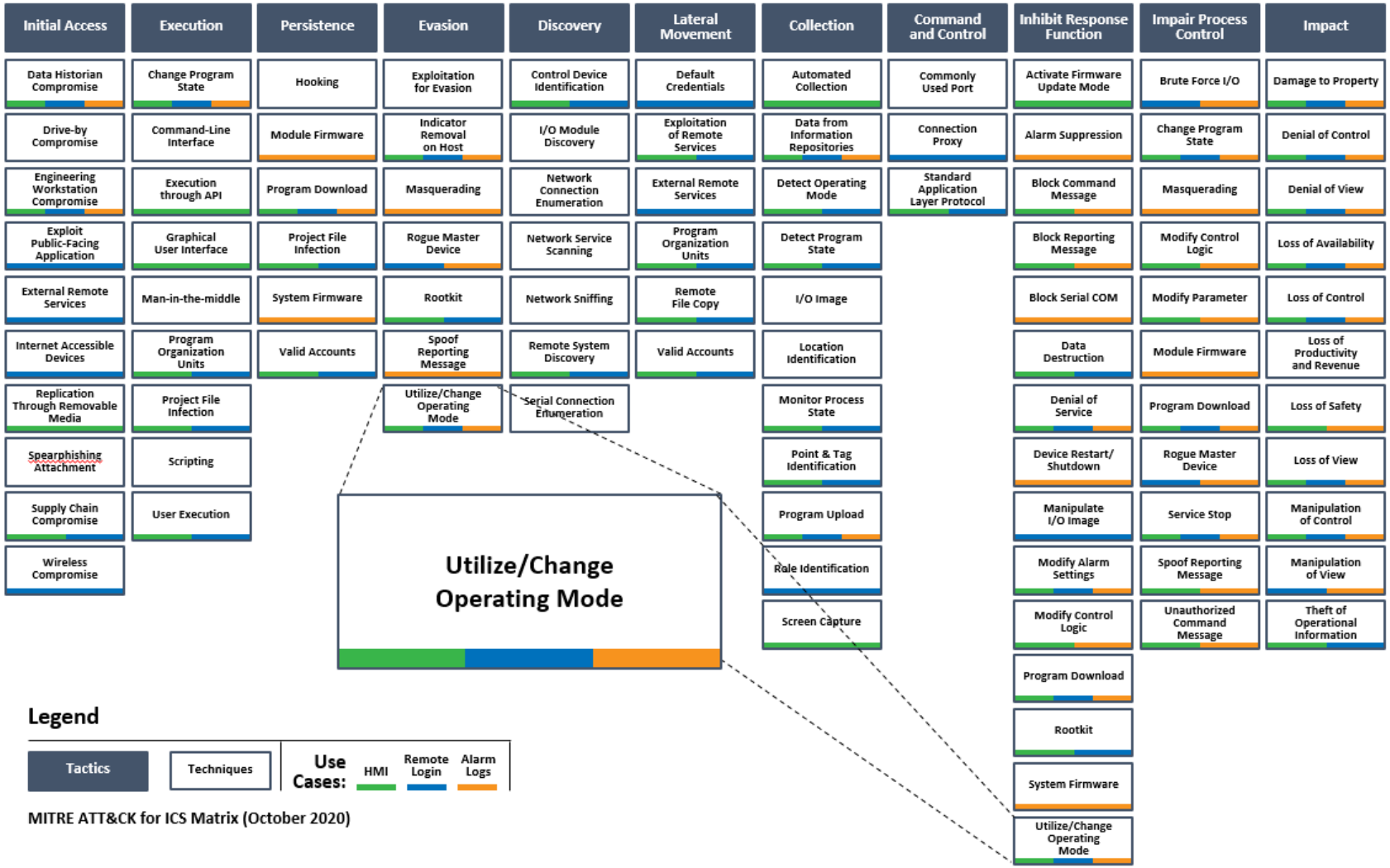

Figure 1: ICS ATT&CK Framework[8] – Utilize/Change Operating Mode Technique

[8] © 2020 The MITRE Corporation. This work is reproduced and distributed with the permission of The MITRE Corporation.